Networks Fundamentals II Homework: *In a Network Far, Far Away!*

Background

- You are a Network Jedi working for the Resistance.
- The Sith Empire recently carried out a DoS attack, taking out the Resistance's core network infrastructure, including its DNS servers.
- This attack destroyed the Resistance's ability to communicate via email and retrieve other crucial information about each others' operations. The Empire has taken advantage of this compromised availability by ambushing numerous Resistance outposts, all vulnerable because they can no longer call for help.
- Your task is a crucial one: Restore the Resistance's core DNS infrastructure and verify that traffic is routing as expected.

Good luck and may the Force be with you!

Files Required

- Darkside pcap
- Galaxy Network Map

Your Objectives:

- Review each network issue in the missions below.
- Document each DNS record type found.
- Take note of the DNS records that can explain the reasons for the existing network issue.
- Provide recommended fixes to save the Galaxy!

Submit your results and findings in a document.

Topics Covered in Your Assignments

- DNS
- NSLOOKUP
- DNS record types
    - `A`, `PTR`, `MX`, `NS`, `SOA`, `SRV`, `TXT`
- Wireless
    - `WEP`, `WPA`
- Aircrack-ng
- Wireshark Wireless analysis and decryption

Mission 1

Issue: Due to the DoS attack, the Empire took down the Resistance's DNS and primary email servers.

- The Resistance's network team was able to build and deploy a new DNS server and mail server.
- The new primary mail server is `asltx.1.google.com` and the secondary should be `asltx.2.google.com`.
- The Resistance (starwars.com) is able to send emails but unable to receive any.

Your mission:

- Determine and document the mail servers for starwars.com using NSLOOKUP.

nslookup -type=MX starwars.com

Server: mygateway

Address: 10.0.0.138

Non-authoritative answer:

starwars.com MX preference = 5, mail exchanger = alt1.aspx.l.google.com

starwars.com MX preference = 1, mail exchanger = aspmx.l.google.com

starwars.com MX preference = 5, mail exchanger = alt2.aspmx.l.google.com

starwars.com MX preference = 10, mail exchanger = aspmx3.googlemail.com

starwars.com MX preference = 10, mail exchanger = aspmx2.googlemail.com

- Explain why the Resistance isn't receiving any emails.

The mail exchange in DNS has not changed from before the mail server and DNS server were changed.

- Document what a corrected DNS record should be.

· starwars.com MX preference = 1, mail exchanger = `asltx.1.google.com`

· starwars.com MX preference = 5, mail exchanger = `asltx.2.google.com`

Mission 2

Issue: Now that you've addressed the mail servers, all emails are coming through. However, users are still reporting that they haven't received mail from the `theforce.net` alert bulletins.

- Many of the alert bulletins are being blocked or going into spam folders.
- This is probably due to the fact that `theforce.net` changed the IP address of their mail server to `45.23.176.21` while your network was down.
- These alerts are critical to identify pending attacks from the Empire.

Your mission:

- Determine and document the `SPF` for `theforce.net` using NSLOOKUP.

  nslookup -type=SPF theforce.com

  unknown query type: SPF

  Server: mygateway

  Address: 10.0.0.138

  Non-authoritative answer:

  Name: theforce.com

  Address: 144.208.74.49

  You used the incorrect type and should be theforce.net. The command should be ‘nslookup -type=txt theforce.net

- Explain why the Force's emails are going to spam.

The new mail server is not recognised by DNS due to the SPF record only recognising the old server.

- Document what a corrected DNS record should be.

Text= "v=spf1 ip4: **`45.23.176.21`** +a +mx +ip4:192.185.150.68 +ip4:184.173.239.120 +include:websitewelcome.com -all"

Right change, wrong record.

Mission 3

Issue: You have successfully resolved all email issues and the resistance can now receive alert bulletins. However, the Resistance is unable to easily read the details of alert bulletins online.

- They are supposed to be automatically redirected from their sub page of `resistance.theforce.net` to `theforce.net`.

Your mission:

- Document how a CNAME should look by viewing the CNAME of `www.theforce.net` using NSLOOKUP.

nslookup -type=CNAME www.theforce.net

Server: mygateway

Address: 10.0.0.138

Non-authoritative answer:

www.theforce.net canonical name = theforce.net

- Explain why the sub page of `resistance.theforce.net` isn't redirecting to `theforce.net`.

  Resistance.theforce.net is not a CNAME for www.force.net

- Document what a corrected DNS record should be.

`www.theforce.net  Canonical name = resistance.theforce.net`

Mission 4

Issue: During the attack, it was determined that the Empire also took down the primary DNS server of `princessleia.site`.

- Fortunately, the DNS server for `princessleia.site` is backed up and functioning.
- However, the Resistance was unable to access this important site during the attacks and now they need you to prevent this from happening again.
- The Resistance's networking team provided you with a backup DNS server of: `ns2.galaxybackup.com`.

Your mission:

- Confirm the DNS records for `princessleia.site`.

  nslookup -type=TXT princessleia.site (or could just use nslookup -type=NS princessleia.site but TXT gives the same info)

  Server: mygateway

  Address: 10.0.0.138

  Non-authoritative answer:

  princessleia.site text =

  "Run the following in a command line: telnet towel.blinkenlights.nl or as a backup access in a browser: www.asciimation.co.nz"

  princessleia.site nameserver = ns26.domaincontrol.com

  princessleia.site nameserver = ns25.domaincontrol.com

  TXT doesn't give the same info as NS

- Document how you would fix the DNS record to prevent this issue from happening again.

Assuming the current Name Servers are ok, add `ns2.galaxybackup.com` to the DNS record. NS lookup will show the new backup Name Server.

princessleia.site nameserver = ns26.domaincontrol.com

princessleia.site nameserver = ns25.domaincontrol.com

princessleia.site namesever = `ns2.galaxybackup.com`

Mission 5

Issue: The network traffic from the planet of `Batuu` to the planet of `Jedha` is very slow.

- You have been provided a network map with a list of planets connected between `Batuu` and `Jedha`.
- It has been determined that the slowness is due to the Empire attacking `Planet N`.

Your Mission:

- View the Galaxy Network Map and determine the `OSPF` shortest path from `Batuu` to `Jedha`.

  Batuu, D, C, G, O, R,V, Jedha = path length 29

- Confirm your path doesn't include `Planet N` in its route.

  No it does not

- Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic.

Shortest path: Batuu, D, C, G, O, R,V, Jedha = path length 31

Incorrect. The shortest path is: Batuu > D > C > E > F > J > I > L > Q > T > V > Jedha with a length of 23

Mission 6

Issue: Due to all these attacks, the Resistance is determined to seek revenge for the damage the Empire has caused.

- You are tasked with gathering secret information from the Dark Side network servers that can be used to launch network attacks against the Empire.
- You have captured some of the Dark Side's encrypted wireless internet traffic in the following pcap: Darkside.pcap.

Your Mission:

- Figure out the Dark Side's secret wireless key by using Aircrack-ng.
    - Hint: This is a more challenging encrypted wireless traffic using WPA.
    - In order to decrypt, you will need to use a wordlist (-w) such as `rockyou.txt`.

```
aircrack-ng -w rockyou.txt Darkside.pcap

Opening Darkside.pcap

Read 586 packets.


  #  BSSID              ESSID                     Encryption


  1  00:0B:86:C2:A4:85  linksys                   WPA (1 handshake)


Choosing first network as target.


Opening Darkside.pcap

Reading packets, please wait...


                                Aircrack-ng 1.2 rc4


                  [00:00:01] 2296/7120714 keys tested (1611.75 k/s)
```

Time left: 1 hour, 13 minutes, 38 seconds 0.03%

KEY FOUND! [dictionary]

Master Key : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2

52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

Transient Key : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC

55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0

A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49

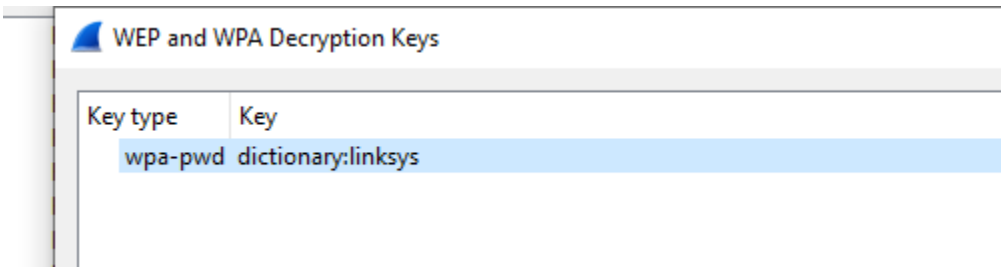
5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

EAPOL HMAC : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51

KEY is dictionary

Next time, use a screenshot instead of copying and pasting the output.

- Use the Dark Side's key to decrypt the wireless traffic in Wireshark.
  - Hint: The format for the key to decrypt wireless is `<Wireless_key>:<SSID>`.



- Once you have decrypted the traffic, figure out the following Dark Side information:
    - Host IP Addresses and MAC Addresses by looking at the decrypted `ARP` traffic.
    - Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.

Darkside MAC address 00:13:ce:55:98:ef

Darkside IP Address 172.16.0.101

There is another pair of IP and MAC addresses that you have missed. This section could benefit with a screenshot of where you found the addresses in Wireshark.

Mission 7

As a thank you for saving the galaxy, the Resistance wants to send you a secret message!

Your Mission:

- View the DNS record from Mission #4.
- The Resistance provided you with a hidden message in the `TXT` record, with several steps to follow.
- Follow the steps from the `TXT` record.
    - **Note**: A backup option is provided in the TXT record (as a website) in case the main telnet site is unavailable
- Take a screen shot of the results.

  Telnet did not work so used the URL www.asciimation.co.nz

Conclusion

- Submit your results and findings from every mission.
- Congratulations, you have completed your mission and saved the Galaxy!